



## Using the Web-Browser Interface

---

This chapter describes the web-browser interface that you can use to configure the access point/bridge. It contains these sections:

- [Using the Web-Browser Interface for the First Time, page 3-2](#)
- [Using the Management Pages in the Web-Browser Interface, page 3-2](#)
- [Enabling HTTPS for Secure Browsing, page 3-4](#)
- [Using Online Help, page 3-12](#)
- [Disabling the Web-Browser Interface, page 3-14](#)

The web-browser interface contains management pages that you use to change access point/bridge settings, upgrade firmware, and monitor and configure other wireless devices on the network.



---

**Note**

The access point/bridge web-browser interface is fully compatible with these browsers: Microsoft Internet Explorer versions 6.0 on Windows 98, 2000, and XP platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

---



---

**Note**

Avoid using the CLI and the web-browser interfaces to configure the access point/bridge. Use one or the other. If you configure the access point/bridge using the CLI, the web-browser interface might display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the access point/bridge is misconfigured.

---

## Using the Web-Browser Interface for the First Time

Use the access point/bridge's IP address to browse to the management system. See the “[Obtaining and Assigning an IP Address](#)” section on page 2-2 for instructions on assigning an IP address to the access point/bridge.

Follow these steps to begin using the web-browser interface:

- 
- Step 1** Start the browser.
  - Step 2** Enter the access point/bridge's IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer) and press **Enter**.
  - Step 3** Enter the administrator username and password and press **Enter**. The default username is *Cisco* and the default password is *Cisco*. The Summary Status page appears.
- 

## Using the Management Pages in the Web-Browser Interface

The system management pages use consistent techniques to present and save configuration information. A navigation bar is on the left side of the page, and configuration action buttons appear at the bottom. You use the navigation bar to browse to other management pages, and you use the configuration action buttons to save or cancel changes to the configuration.

**Note**

---

It is important to remember that clicking your browser's **Back** button returns you to the previous page without saving any changes you have made. Clicking **Cancel** cancels any changes you made on the page and keeps you on that page. Changes are only applied when you click **Apply**.

---

[Figure 3-1](#) shows the web-browser interface home page.

**Figure 3-1** Web-Browser Interface Home Page

The screenshot shows the Web-Browser Interface Home Page for a bridge. The page title is "Home: Summary Status" and the hostname is "bridge". The bridge uptime is 47 minutes. The page is divided into several sections:

- Navigation Menu:** HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, EVENT LOG.
- Summary Status:**
  - Association:** Clients: 0, Infrastructure clients: 0
  - Network Identity:** IP Address: 10.0.0.1, MAC Address: 0005.9a3f.57f4
  - Network Interfaces:**

Interface	MAC Address	Transmission Rate
FastEthernet	0005.9a3f.57f4	100Mb/s
Radio0-802.11G	000e.8319.2800	54.0Mb/s
  - Event Log:**

Time	Severity	Description
Mar 1 00:01:40.876	Notification	Line protocol on Interface Dot11Radio0, changed state to up
Mar 1 00:01:39.882	Error	Interface Dot11Radio0, changed state to up
Mar 1 00:01:39.875	Warning	Root selected
Mar 1 00:00:50.307	Warning	Interface Dot11Radio0, cannot associate: No matching SSID
Mar 1 00:00:40.355	Notification	Interface Dot11Radio0, changed state to reset
Mar 1 00:00:40.354	Warning	Non-root - scanning for root
Mar 1 00:00:34.307	Information	Interface Dot11Radio0, frequency 2447 selected
Mar 1 00:00:26.409	Notification	Line protocol on Interface Dot11Radio0, changed state to down
Mar 1 00:00:26.375	Notification	Line protocol on Interface BV11, changed state to up
Mar 1 00:00:25.448	Notification	Interface Dot11Radio0, changed state to administratively down

A "Refresh" button is located at the bottom right of the page.

117034

## Using Action Buttons

Table 3-1 lists the page links and buttons that appear on most management pages.

**Table 3-1** Common Buttons on Management Pages

Button/Link	Description
<b>Navigation Links</b>	
Home	Displays access point/bridge status page with information on the number of radio devices associated to the access point/bridge, the status of the Ethernet and radio interfaces, and a list of recent access point/bridge activity.
Express Setup	Displays the Express Setup page that includes basic settings such as system name, IP address, and SSID.
Express Security	Displays the Express Security page from which you can select basic security settings (no security, static WEP key, EAP authentication, or WPA).
Network Map	Displays a list of infrastructure devices on your wireless LAN.
Association	Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.

**Table 3-1 Common Buttons on Management Pages (continued)**

Button/Link	Description
Network Interfaces	Displays status and statistics for the Ethernet and radio interfaces and provides links to configuration pages for each interface.
Security	Displays a summary of security settings and provides links to security configuration pages.
Services	Displays status for several access point/bridge features and links to configuration pages for Telnet/SSH, CDP, domain name server, filters, proxy Mobile IP, QoS, SNMP, SNTP, and VLANs.
Wireless Services	Displays the Wireless Domain Services Status page and provides access to the AP and Wireless Domain Services (WDS) pages.
System Software	Displays the version number of the firmware that the access point/bridge is running and provides links to configuration pages for upgrading and managing firmware.
Event Log	Displays the access point/bridge event log and provides links to configuration pages where you can select events to be included in traps, set event severity levels, and set notification methods.
<b>Configuration Action Buttons</b>	
Apply	Saves changes made on the page and remains on the page.
Refresh	Updates status information or statistics displayed on a page.
Cancel	Discards changes to the page and remains on the page.
Back	Discards any changes made to the page and returns to the previous page.

## Character Restrictions in Entry Fields

Because the 1300 series access point/bridge uses Cisco IOS software, there are certain characters that you cannot use in the entry fields on the web-browser interface. You cannot use these characters in entry fields:

“  
]  
+  
/  
Tab  
Trailing space

## Enabling HTTPS for Secure Browsing

You can protect communication with the access point/bridge web-browser interface by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol.



### Note

When you enable HTTPS, your browser might lose its connection to the access point/bridge. If you lose the connection, change the URL in your browser's address line from `http://ip_address` to `https://ip_address` and log into the access point again.

**Note**

When you enable HTTPS, most browsers prompt you for approval each time you browse to a device that does not have a fully qualified domain name (FQDN). To avoid the approval prompts, complete [Step 2](#) through [Step 9](#) in these instructions to create an FQDN for the access point. However, if you do not want to create an FQDN, skip to [Step 10](#).

Follow these steps to create an FQDN and enable HTTPS:

- Step 1** If your browser uses popup-blocking software, disable the popup-blocking feature.
- Step 2** Browse to the Express Setup page. [Figure 3-2](#) shows the Express Setup page.

**Figure 3-2** Express Setup Page

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP +  
ASSOCIATION +  
NETWORK INTERFACES +  
SECURITY +  
SERVICES +  
WIRELESS SERVICES +  
SYSTEM SOFTWARE +  
EVENT LOG +

Hostname root root uptime is 5 days, 22 hours, 47 minutes

**Express Set-Up**

**Host Name:**

**MAC Address:** 0012.016c.0240

**Configuration Server Protocol:**  DHCP  Static IP

**IP Address:**

**IP Subnet Mask:**

**Default Gateway:**

**SNMP Community:**

Read-Only  Read-Write

**Radio0-802.11G**

**Role in Radio Network:**  Root  Non-Root  Install-Mode  
 Non-Root with Clients  
 Root AP  Repeater AP  
 Workgroup Bridge

**Optimize Radio Network for:**  Throughput  Range  Default  Custom

**Aironet Extensions:**  Enable  Disable

127769

- Step 3** Enter a name for the access point/bridge in the System Name field and click **Apply**.
- Step 4** Browse to the Services – DNS page. [Figure 3-3](#) shows the Services – DNS page.

Figure 3-3 Services – DNS Page

HOME Hostname root root uptime is 5 days, 22 hours, 16 minutes

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY +

**SERVICES**

Telnet/SSH

CDP

**DNS**

Filters

HTTP

QoS

SNMP

SNTP

VLAN

STP

ARP Caching

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

**Services: DNS - Domain Name Service**

Domain Name System (DNS):  Enable  Disable

Domain Name (optional):

**Name Server IP Addresses:**

1.

2.

3.

Apply Cancel 127775

**Step 5** Select **Enable** for Domain Name System.

**Step 6** In the Domain Name field, enter your company's domain name. At Cisco Systems, for example, the domain name is *cisco.com*.

**Step 7** Enter at least one IP address for your DNS server in the Name Server IP Addresses entry fields.

**Step 8** Click **Apply**. The access point/bridge's FQDN is a combination of the system name and the domain name. For example, if your system name is *br 1310* and your domain name is *company.com*, the FQDN is *br1310.company.com*.

**Step 9** Enter the FQDN on your DNS server.

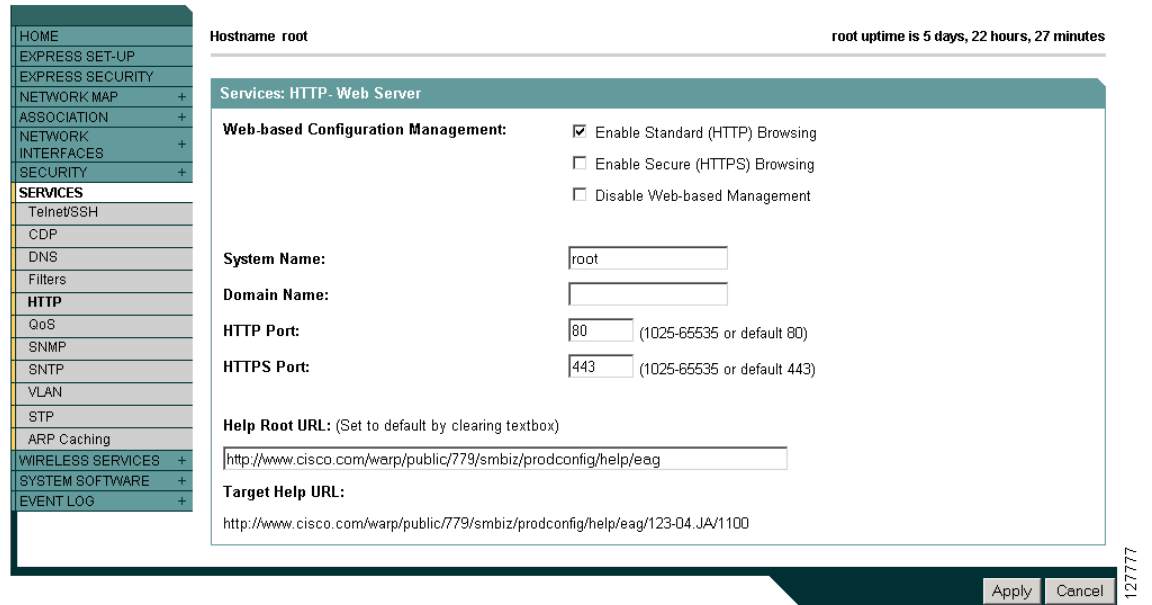


**Tip**

If you do not have a DNS server, you can register the access point/bridge's FQDN with a dynamic DNS service. Search the Internet for *dynamic DNS* to find a fee-based DNS service.

**Step 10** Browse to the Services: HTTP Web Server page. [Figure 3-4](#) shows the HTTP Web Server page:

Figure 3-4 Services: HTTP Web Server Page



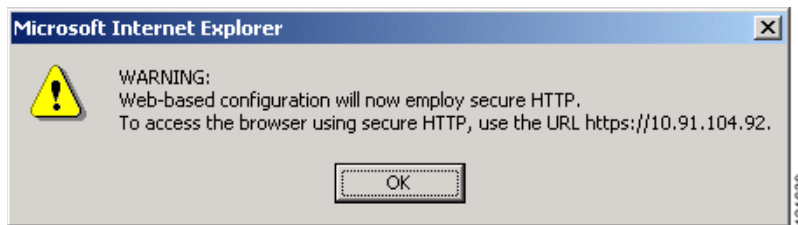
**Step 11** Select the Enable Secure (HTTPS) Browsing check box and click **Apply**.



**Note** Although you can enable both standard HTTP and HTTPS, Cisco recommends that you enable one or the other.

A warning window appears stating that you will use HTTPS to browse to the access point. The window also instructs you to change the URL that you use to browse to the access point/bridge from *http* to *https*. Figure 3-5 shows the warning window:

Figure 3-5 HTTPS Warning Window



**Step 12** Click **OK**. The address in your browser’s address line changes from **http://ip-address** to **https://ip-address**.

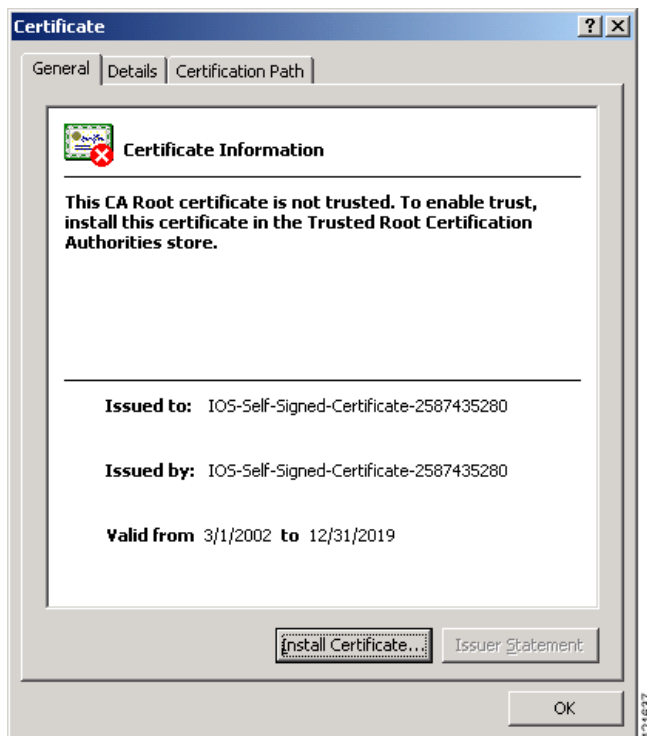
**Step 13** Another warning window appears stating that the access point’s security certificate is valid but is not from a known source. However, you can accept the certificate with confidence because the site in question is your own access point. Figure 3-6 shows the certificate warning window:

**Figure 3-6 Certificate Warning Window**



**Step 14** Click **View Certificate** to accept the certificate before proceeding. (To proceed without accepting the certificate, click **Yes**, and skip to [Step 23](#) in these instructions.) [Figure 3-7](#) shows the Certificate window.

**Figure 3-7 Certificate Window**



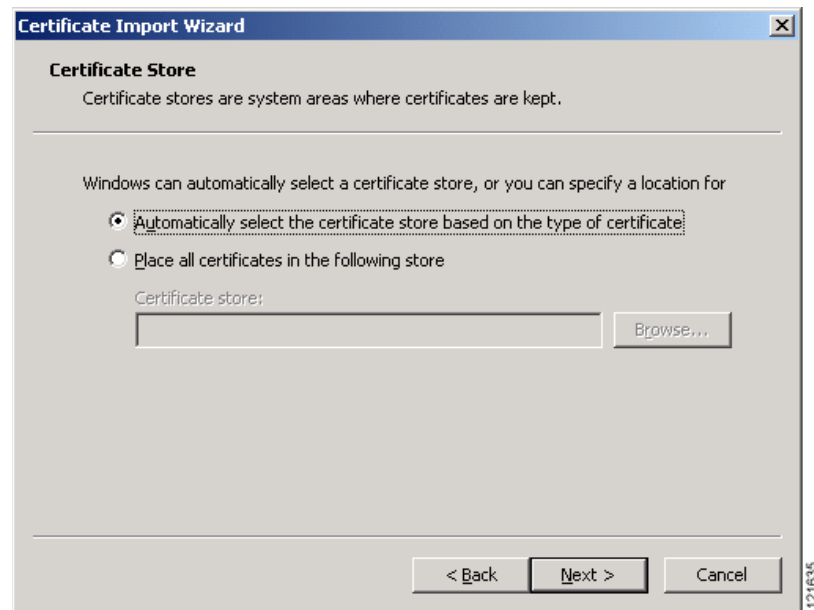
**Step 15** On the Certificate window, click **Install Certificate**. The Microsoft Windows Certificate Import Wizard appears. [Figure 3-8](#) shows the Certificate Import Wizard window.

**Figure 3-8** Certificate Import Wizard Window



- Step 16** Click **Next**. The next window asks where you want to store the certificate. Cisco recommends that you use the default storage area on your system. [Figure 3-9](#) shows the window that asks about the certificate storage area.

**Figure 3-9** Certificate Storage Area Window



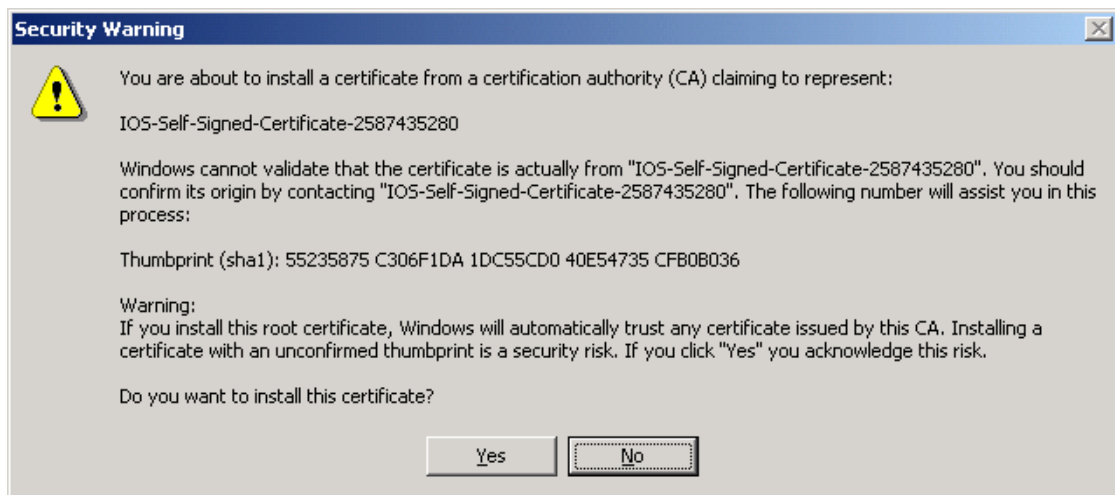
- Step 17** Click **Next** to accept the default storage area. A window appears that states that you successfully imported the certificate. [Figure 3-10](#) shows the completion window.

Figure 3-10 Certificate Completion Window

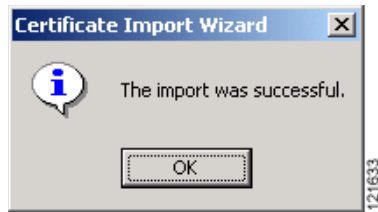


Step 18 Click **Finish**. Windows displays a final security warning. Figure 3-11 shows the security warning.

Figure 3-11 Certificate Security Warning



Step 19 Click **Yes**. Windows displays another window stating that the installation is successful. Figure 3-12 shows the completion window.

**Figure 3-12** *Import Successful Window*

- Step 20** Click **OK**.
- Step 21** On the Certificate window shown in [Figure 3-7](#), which is still displayed, click **OK**.
- Step 22** On the Security Alert window shown in [Figure 3-6](#), click **Yes**.
- Step 23** The access point login window appears and you must log into the access point again. The default user name is *Cisco* (case-sensitive) and the default password is *Cisco* (case-sensitive).

## CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the [“Using Online Help” section on page 3-12](#):

```
ap# configure terminal
ap(config)# hostname br1310
ap(config)# ip domain name company.com
ap(config)# ip name-server 10.91.107.18
ap(config)# ip http secure-server
ap(config)# end
```

In this example, the access point system name is *br1310*, the domain name is *company.com*, and the IP address of the DNS server is 10.91.107.18.

For complete descriptions of the commands used in this example, consult the Cisco IOS Commands Master List, Release 12.3. Click this link to browse to the master list of commands:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123mindx/index.htm>

## Deleting an HTTPS Certificate

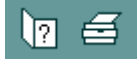
The access point generates a certificate automatically when you enable HTTPS. However, if you need to change the access point’s fully qualified domain name (FQDN) or you need to add an FQDN after enabling HTTPS, you might need to delete the certificate. Follow these steps:

- Step 1** Browse to the Services: HTTP Web Server page.
- Step 2** Uncheck the **Enable Secure (HTTPS) Browsing** check box to disable HTTPS.
- Step 3** Click **Delete Certificate** to delete the certificate.
- Step 4** Re-enable HTTPS. The access point generates a new certificate using the new FQDN.

# Using Online Help

Click the help icon at the top of any page in the web-browser interface to display online help. [Figure 3-13](#) shows the print and help icons.

**Figure 3-13** *Print and Help Icons*



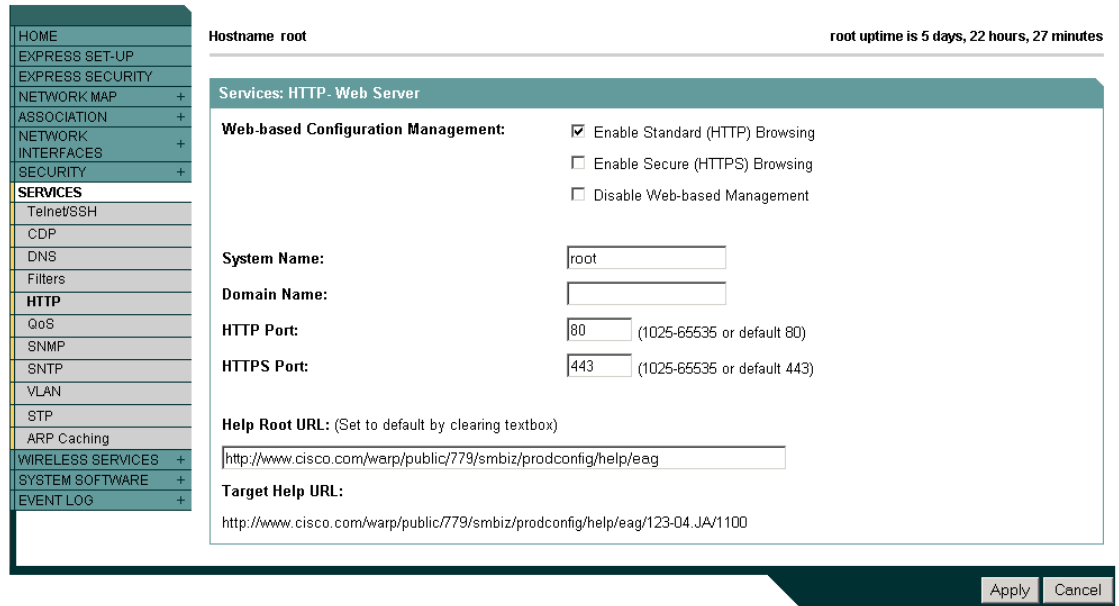
When a help page appears in a new browser window, use the Select a topic drop-down menu to display the help index or instructions for common configuration tasks, such as configuring VLANs.

## Changing the Location of Help Files

Cisco maintains up-to-date HTML help files for access points and bridges on the Cisco web site. By default, the access point/bridge opens a help file on Cisco.com when you click the help button on the access point web-browser interface. However, you can install the help files on your network so your devices can access them there. Follow these steps to install the help files locally:

- 
- Step 1** Download the help files from the Software Center on Cisco.com. Click this link to browse to the Software Center's Wireless Software page:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- Select the help files that match the software version on your access point.
- Step 2** Unzip the help files on your network in a directory accessible to your access point/bridge. When you unzip the help files, the HTML help pages are stored in a folder named according to the help version number and access point model number.
- Step 3** Browse to the Services: HTTP Web Server page in the access point web-browser interface. [Figure 3-14](#) shows the HTTP Web Server page:

Figure 3-14 HTTP Web Server Page



**Step 4** In the Default Help Root URL entry field, enter the complete path to the location where you unzipped the help files. When you click the access point help button, the access point automatically appends the help version number and model number to the path that you enter.



**Note** Do not add the help version number and device model number to the Default Help Root URL entry. The access point automatically adds the help version and model number to the help root URL.

If you unzip the help files on your network file server at `//myserver/myhelp`, your Default Help Root URL looks like this:

`http://myserver/myhelp`

Table 3-2 shows an example help location and Help Root URL for an 1100 series access point.

Table 3-2 Example Help Root URL and Help Location

Files Unzipped at This Location	Default Help Root URL	Actual Location of Help Files
<code>//myserver/myhelp</code>	<code>http://myserver/myhelp</code>	<code>//myserver/myhelp/123-02.JA/1100</code>

**Step 5** Click **Apply**.

# Disabling the Web-Browser Interface

To prevent all use of the web-browser interface, select the **Disable Web-Based Management** check box on the Services: HTTP-Web Server page and click **Apply**. Figure 3-15 shows the Services: HTTP-Web Server page.

**Figure 3-15** Services: HTTP-Web Server Page

HOME Hostname root root uptime is 5 days, 22 hours, 27 minutes

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY +

**SERVICES**

Telnet/SSH

CDP

DNS

Filters

**HTTP**

QoS

SNMP

SNTP

VLAN

STP

ARP Caching

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

**Services: HTTP- Web Server**

**Web-based Configuration Management:**

Enable Standard (HTTP) Browsing

Enable Secure (HTTPS) Browsing

Disable Web-based Management

**System Name:** root

**Domain Name:**

**HTTP Port:** 80 (1025-65535 or default 80)

**HTTPS Port:** 443 (1025-65535 or default 443)

**Help Root URL:** (Set to default by clearing textbox)

http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag

**Target Help URL:**

http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/123-04.JA/1100

Apply Cancel

127777

To re-enable the web-browser interface, enter this global configuration command on the access point CLI:

```
ap(config)# ip http server
```